In-Wall AP Series User Manual

(Applicable to MT-W101, MT-W121, MT-W104G)

V1.0

Maipu Communication Technology Co., Ltd
No. 16, Jiuxing Avenue
Hi-tech Park
Chengdu, Sichuan Province
People's Republic of China - 610041
Tel: (86) 28-85148850, 85148041
Fax: (86) 28-85148948, 85148139
URL: http: // www.maipu.com
Email: overseas@maipu.com

Copyright

Copyright ©2013, Maipu Communication Technology Co., Ltd.   All Rights Reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Maipu Communication Technology Co., Ltd.

MAIPU and 迈普 are trademarks of Maipu Communication Technology Co., Ltd.

All other trademarks that may be mentioned in this manual are the property of their respective owners.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied.

Security Statement

Important! Before powering on and starting the product, please read the security and compatibility information of the product.

Environmental protection

This product has been designed to comply with the environmental protection requirements. The storage, use, and disposal of this product must meet the applicable national laws and regulations.

Preface

Thank you for using Maipu high-performance wireless access point (AP). The AP is the next-generation wireless access point of high performance based on 802.11n and can provide the wireless access rate six times of the traditional 802.11a/b/g. In addition, the AP can cover more extensive area.

The AP supports both the Fat and Fit work mode and can switch flexibly between these two modes as required by the network planning. The AP needs to cooperate with the wireless network controller when acting as a fit AP and can be deployed independently when acting as a fat AP. By supporting the Fat and Fit work modes, the AP can be smoothly upgraded to the large-scale network from the small-size WLAN network. This can greatly protect the user investment.

The AP works at the 2.4GHz band and adopts the MIMO and OFDM technologies. The AP can provide the data transmission rate with a maximum of 150 Mbps for single channel and a maximum of 300 Mbps for the dual-channel.

In addition, the AP has the comfortable interface and combines the simple interface, which enables the user to complete the setting quickly and enables the user to use the AP more convenient and efficient.

Chapter 1: product overview, briefly describes the main AP feature and product specifications.

Chapter 2: detailed configuration guide, instructs you to configure the AP parameters and advanced features.

Contents

1 Product Introduction

1.1 Overview

The AP is the next-generation wireless access point of high performance based on 802.11n and can provide the wireless access rate six times of the traditional 802.11a/b/g. In addition, the AP can cover more extensive area.

The AP supports both the Fat and Fit work mode and can switch flexibly between these two modes as required by the network planning. MP101 needs to cooperate with the wireless network controller when acting as a fit AP and can be deployed independently when acting as a fat AP. By supporting the Fat and Fit work modes, the AP can be smoothly upgraded to the large-scale network from the small-size WLAN network. This can greatly protect the user investment.

The AP works at the 2.4GHz band and adopts the MIMO and OFDM technologies. The AP can provide the data transmission rate with a maximum of 150 Mbps for single channel and a maximum of 300 Mbps for the dual-channel.

1.2 Main Features and Specifications

1.2.1 Main Features

Easy to deploy

The AP can automatically detect the AC and delivers the configuration via the AC. The wireless network can be enabled for the AP zero configuration. The AP can integrate with the existing AP, firewall, authentication server, and other network architecture seamlessly without changing the existing network architecture.

High-rate broadband wireless access

The AP supports 802.11a/b/g/n and works at the 2.4GHz band, providing high-rate wireless access service of high quality for users.

Centralized management

The AP can act as a fit AP and cooperate with the AC. The AC uniformly controls all the fit APs in the network and the status of all the devices can be viewed. Comparing with the traditional fat AP, the AC and the fit AP application mode greatly facilitate the administrator to manage the entire network.

AP centralized upgrade

The AP can achieve the centralized management by the wireless network controller in the network and uniformly upgrade the AP to the latest version. The AP can apply new firmware automatically without manual interference, which reduces the workload of network maintenance. The feature is especially important to the large-scale network.

User isolation policy

The AP supports the isolation between the wireless users. When this function enabled, two wireless clients cannot communicate directly. The wireless client can intelligently visit the upstream wired network. When applying this feature, the carrier can force the wireless user to the specified gateway or server for billing or more secure authentication, realizing the hotpot application.

Multiple forms and convenient installation

This series APs have multiple form design and can be applicable to different installation scenarios. There is no need to smash the wall to lay out cables and furnish the wall for the second time. The AP provides the wireless coverage based on the wired network and can be installed conveniently and quickly. Cooperating with the wireless network controller, the wireless AP can achieve plug-and-play and AP zero configuration, and all the AP management, control, and configuration are completed by the AC. The network management personnel does not need to manage and maintain the mass of APs one by one, and all actions, such as the configuration, firmware upgrade, and security policy update can be delivered uniformly by the AC.

2 Detailed Configuration Guide

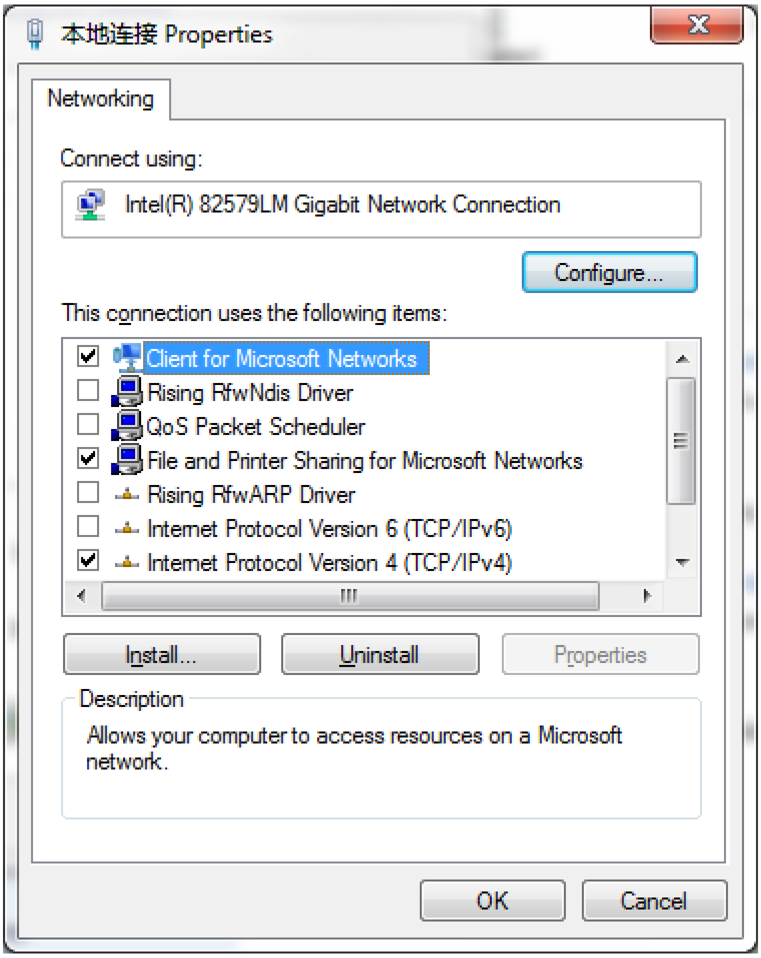
2.1 PC Configuration

To facilitate the user management, the AP integrates the web management function. Through this function, we can realize various management functions in a simple mode to facilitate using. When the user configures the hardware, the user can use the PC to configure the AP.

Through the PC connected to the AP, the user can easily perform the web management after the following configuration.

The default IP address of the AP is 192.168.170.1 and this parameter can be set as required. The following takes the default value as an example. The PC is set by the following steps:

1) Connect the PC to the port of the AP.
2) Set the IP address of the PC.
3) Select **Network** > **Network** > **Local Connection**.
4) Right-click **Local Connection** and click **Properties** on the displayed menu.
5) Select **Internet Protocol Version 4 (TCP/IPv4)**, as shown in Figure 2-1.



本地连接 Properties

Networking

Connect using:

Intel(R) 82579LM Gigabit Network Connection

This connection uses the following items:

- ☑ Client for Microsoft Networks
- □ Rising RfwNdis Driver
- □ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- □ Rising RfwARP Driver
- □ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)

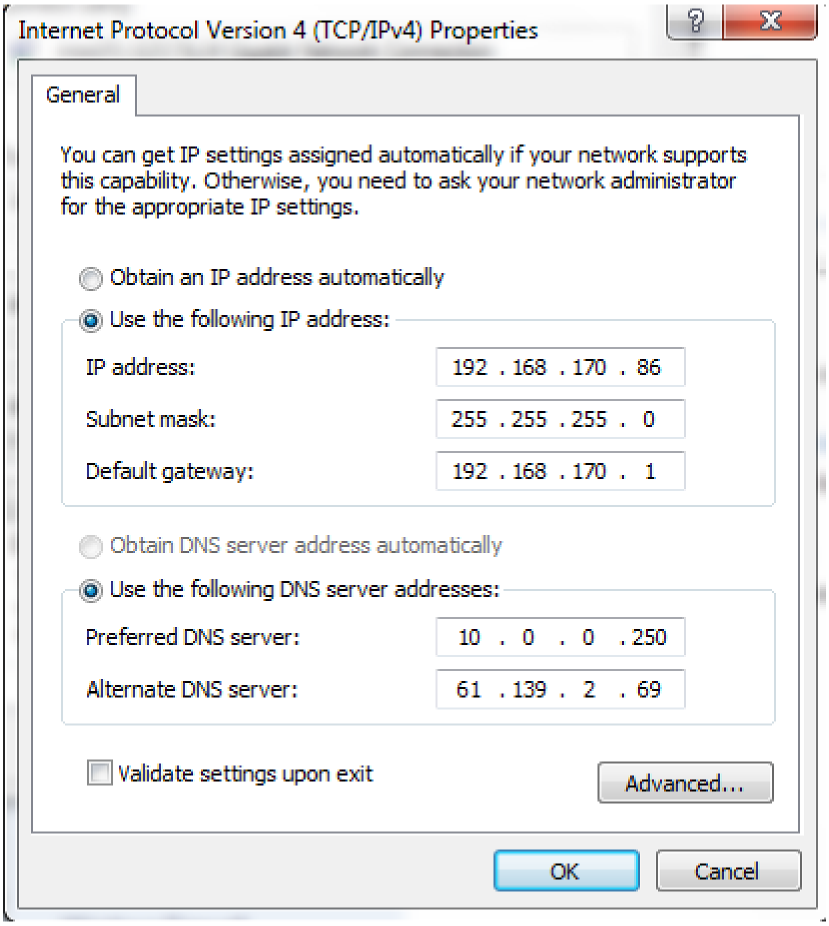
Description

Allows your computer to access resources on a Microsoft network.

Figure 2-1 Select Internet TCP/IP protocol on the attribute window

Click **Properties** to set the IP address of the PC.

On the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box, choose **Use the following IP address** and input 192.168.170.xxx in **IP address**, 255.255.255.0 in **Subnet mask**, and input 192.168.170.1 (default IP address of the AP) in **Default gateway**.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 170 . 86

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 170 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 10 . 0 . 0 . 250

Alternate DNS server: 61 . 139 . 2 . 69

□ Validate settings upon exit

Figure 2-2 Input IP address on the TCP/IPv4 attribute interface

1) Click **OK** to complete the configuration.
2) Test whether the PC is connected to the AP.
3) Choose **Start** > **Run**. Input **cmd** > and click **OK**.
4) Execute the ping command in command prompt to test whether the connection succeeds.
5) Ping 192.168.170.1.

The result is displayed, as shown in Figure 2-3.

```
Pinging 192.168.170.1 with 32 byte of data:
Replyfrom 192.168.170.1:bytes=32 time<10ms TTL=64
Replyfrom 192.168.170.1:bytes=32 time<10ms TTL=64
Replyfrom 192.168.170.1:bytes=32 time<10ms TTL=64
Replyfrom 192.168.170.1:bytes=32 time<10ms TTL=64

Ping statistics for 192.168.170.1:
Packets:Sent=4,Received=4,Lost=0(0% loss).
```

Figure 2-3 Connection success between the PC and AP

If the information in Figure 2-3 is displayed, it indicates that the connection succeeds.

The result may also be displayed, as shown in Figure 2-4.

```
Pinging 192.168.170.1 with 32 byte of data:


Requesttimed out.

Requesttimed out.

                              Requesttimed out.


Ping statistics for 192.168.170.1:

Packets:Sent=4,Received=4,Lost=0(100% loss).
```

Figure 2-4 Connection failure between the PC and AP

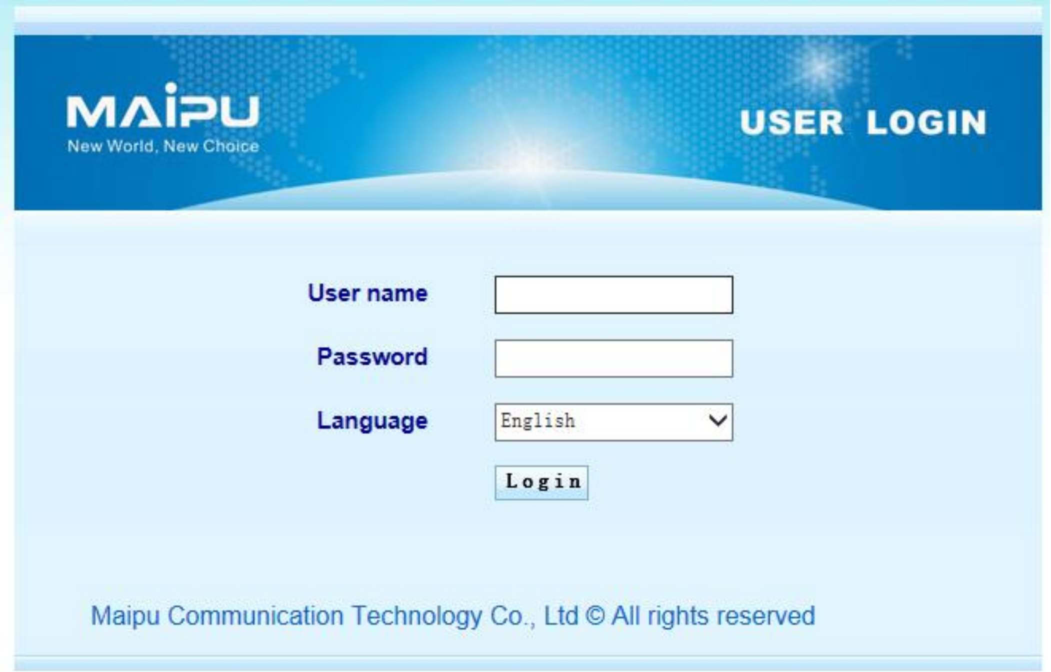
If the information in Figure 2-4 is displayed, it indicates that the PC is not correctly connected to the AP.

In this case, you should check:

1) Check whether the indicator is on.
2) Check whether the TCP/IP is correctly filled.

2.2 System Login

The AP provides the local and remote web management. Input http://192.168.170.1 in the address bar of the Internet browser to log in to the AP configuration interface. The login interface is displayed, as shown in Figure 2-5.



USER LOGIN

User name

Password

Language English

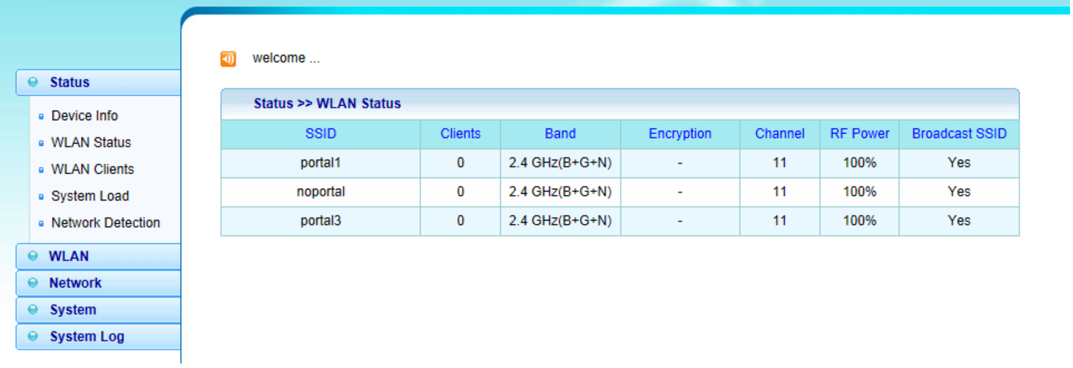
Login

Maipu Communication Technology Co., Ltd © All rights reserved

Figure 2-5 The AP configuration interface

Both the default user name and password of the AP are ***admin*** and the default IP address is 192.168.170.1.

After correctly logging in to the system, the homepage is displayed, as shown in Figure 2-6. The homepage may vary slightly for different models.



welcome ...

Status >> WLAN Status

SSID	Clients	Band	Encryption	Channel	RF Power	Broadcast SSID
portal1	0	2.4 GHz(B+G+N)	-	11	100%	Yes
noportal	0	2.4 GHz(B+G+N)	-	11	100%	Yes
portal3	0	2.4 GHz(B+G+N)	-	11	100%	Yes

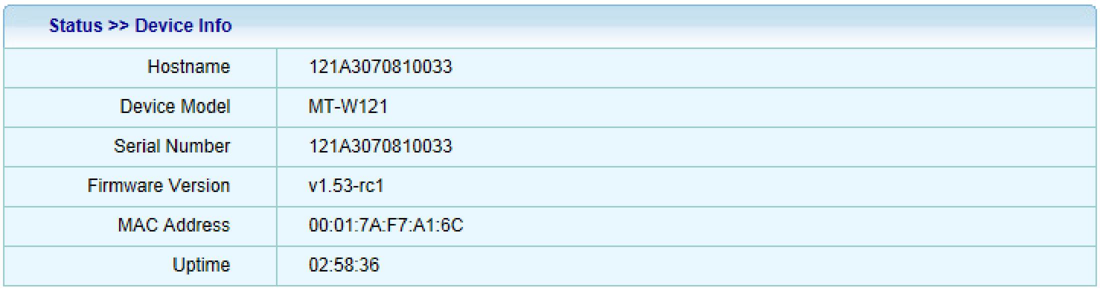
Figure 2-6 The homepage displayed after logging in to the system

The homepage displays the system wireless status of the device, including the SSID containing APs and number of connected APs.

2.3 System Status

2.3.1 Device Information

On the **Device Info** interface, the device information of the AP, including **Hostname**, **Device Model**, **Serial Number**, **Firmware Version**, **MAC Address**, and **Uptime**, is displayed as shown in Figure 2-7.



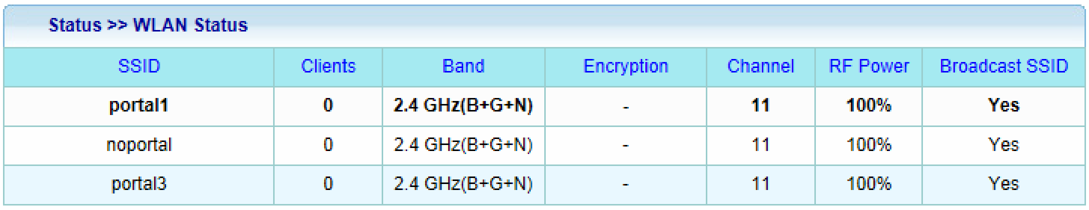
Status >> Device Info

Hostname	121A3070810033
Device Model	MT-W121
Serial Number	121A3070810033
Firmware Version	v1.53-rc1
MAC Address	00:01:7A:F7:A1:6C
Uptime	02:58:36

Figure 2-7 The device information interface

2.3.2 WLAN Status

On the **WLAN Status** interface, the status information of the AP wireless connection, including **SSID**, **Encryption**, **Band**, **Channel**, and **Broadcast SSID**, is displayed as shown in Figure 2-8.



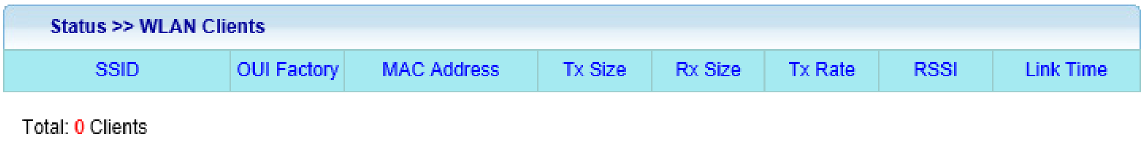
Status >> WLAN Status

SSID	Clients	Band	Encryption	Channel	RF Power	Broadcast SSID
portal1	**0**	**2.4 GHz(B+G+N)**	-	**11**	**100%**	**Yes**
noportal	0	2.4 GHz(B+G+N)	-	11	100%	Yes
portal3	0	2.4 GHz(B+G+N)	-	11	100%	Yes

Figure 2-8 The WLAN status interface

2.3.3 WLAN Client

On the **WLAN Clients** interface, the information of the host that is successfully connected to the AP can be viewed, as shown in Figure 2-9.



Status >> WLAN Clients

SSID	OUI Factory	MAC Address	Tx Size	Rx Size	Tx Rate	RSSI	Link Time

Total: 0 Clients

Figure 2-9 The WLAN client information

(1) **MAC Address**: specifies the MAC address of the host that is successfully connected to the AP.

(2) **Tx Size**: specifies the data traffic that sent by the host.

(3) **Rx Size**: specifies the data traffic received by the host.

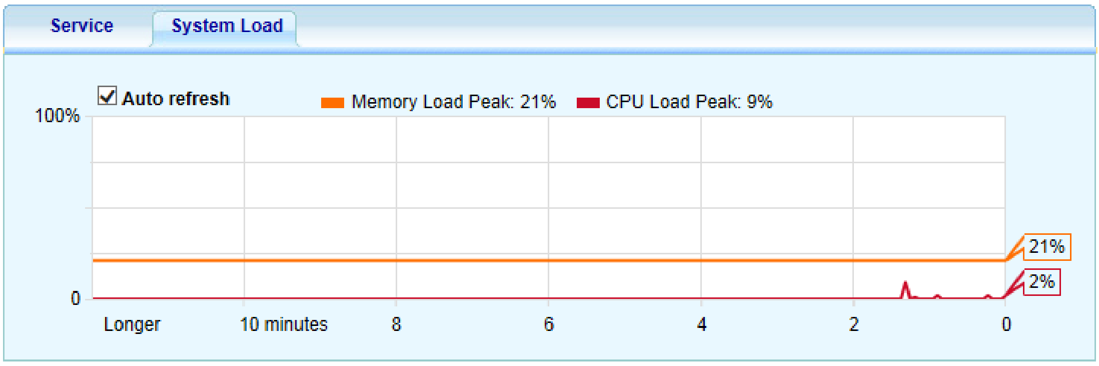
(4) **Tx Rate**: specifies the current rate of sending data package by the host.

(5) **RSSI**: specifies the signal strength between the host and the AP.

(6) **Link Time**: specifies the time that the host is connected to the AP.

2.3.4 System Load

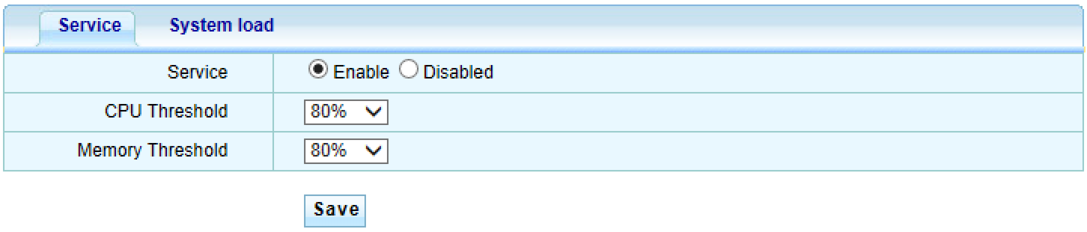
On the **System Load** interface, you can view the current AP memory and CPU load, as shown in Figure 2-10.



☑ Auto refresh

Memory Load Peak: 21%

CPU Load Peak: 9%



Service	● Enable ○ Disabled
CPU Threshold	80%
Memory Threshold	80%

Figure 2-10 The system load interface

(1) **Auto refresh**: specifies whether to automatically refresh the current system load status.

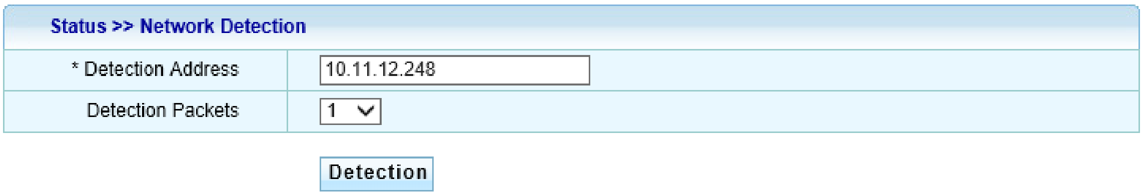
(2) **Service**: specifies whether to enable the system load alarm mechanism.

CPU Threshold: specifies the CPU alarm threshold.

Memory Threshold: specifies the memory alarm threshold.

2.3.5 Network Detection

On the detection interface, you can detect the network connection status（ping test is used here.）, as shown in Figure 2-11.



Status >> Network Detection

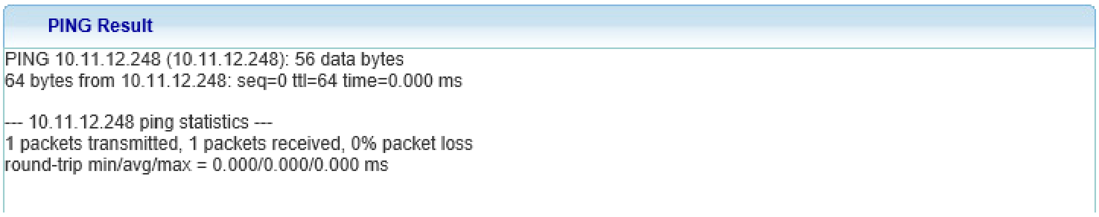
* Detection Address	10.11.12.248
Detection Packets	1

Figure 2-11 The ping detection interface

(1) **Detection Address**: specifies the target host for the system sending the ICMP packet.

(2) **Detection Packets**: specifies the number of ICMP packets sent by the system. The number must an integer from 1 to 10.

(3) **Detection**: notifies the system to begin to send the ICMP packet.



PING Result

```
PING 10.11.12.248 (10.11.12.248): 56 data bytes
64 bytes from 10.11.12.248: seq=0 ttl=64 time=0.000 ms

--- 10.11.12.248 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.000/0.000/0.000 ms
```

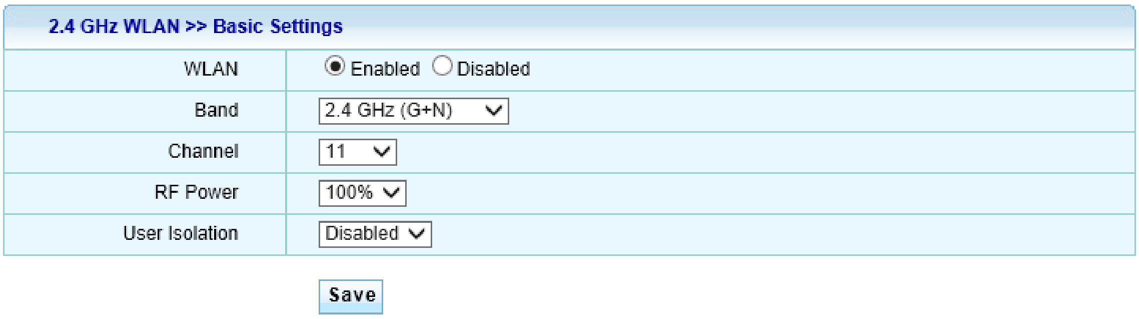
Figure 2-12 The result of network detection.

2.4 Wireless Configuration

2.4.1 Wireless Parameter

On the **Basic Settings** interface, you can configure SSID, network band, and network channel of the AP.

Choose **WEB Management** > **2.4 GHz WLAN** > **Basic Settings** to enter the **Basic Settings** interface, as shown in Figure 2-13.



2.4 GHz WLAN >> Basic Settings

WLAN	● Enabled ○ Disabled
Band	2.4 GHz (G+N)
Channel	11
RF Power	100%
User Isolation	Disabled

Figure 2-13 The wireless parameter interface

(1) **WLAN**: specifies whether to enable or disable the wireless network function of the AP.

(2) **Band**: specifies the network protocol mode that the AP works at. Currently, the AP supports the combination of the 802.11B, 802.11G, 802.11N, B+G, G+N, and B+G+N six protocols.

(3) **Channel**: indicates the wireless channel. It is the data signal transmission channel considering the wireless signal as transmission media. When multiple devices exist in the area covered by the AP signal, set different channels to avoid interference. The AP has a total of 1 to 11 channels.

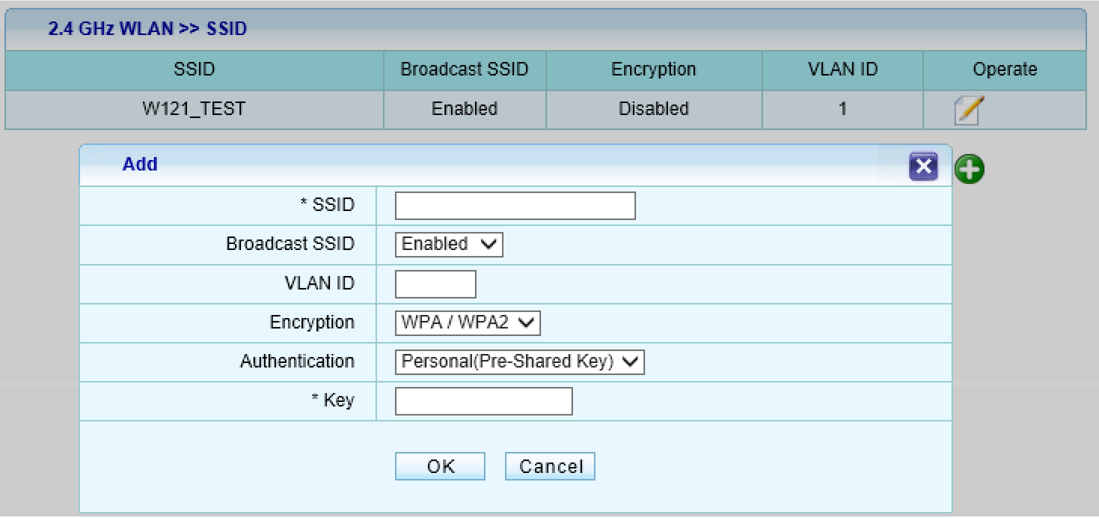
(4) **RF Power**: adjusts the output power of the AP.

(5) **User Isolation**: the wireless clients cannot communicate with each other when the function is enabled.

2.4.2 SSID

On the **Add** interface, you can configure the SSID information of the AP.

Choose **WEB Management** > **2.4GHz WLAN** > **SSID** to enter the **Add** interface, as shown in Figure 2-14.



2.4 GHz WLAN >> SSID

SSID	Broadcast SSID	Encryption	VLAN ID	Operate
W121_TEST	Enabled	Disabled	1	✎

Add

* SSID	
Broadcast SSID	Enabled
VLAN ID	
Encryption	WPA / WPA2
Authentication	Personal(Pre-Shared Key)
* Key	

Figure 2-14 The adding SSID interface

(1) **SSID**: short for Service Set Identifier, can divide a WLAN into several subnetworks requiring different authentications. Each subnetwork needs independent authentication and only users passing the authentication can enter the corresponding subnetwork. This can prevent the unauthorized users entering this network. That is to say, SSID is the name of your network.

(2) **Broadcast SSID**: specifies whether to allow the wireless network to be searched by others through the SSID name. When this function is disabled, the wireless network is still available, but it will not be searched in others' available network list and the wireless network efficiency will be affected to a certain extent.

(3) **VLAN ID**: specifies the VLAN ID to be allocated to the AP.

(4) **Encryption**: specifies whether to encrypt the set SSID. The AP provides the WEP, WPA, WPA2, and WPA/WPA2 four encryption modes.

WEP: short for Wired Equivalent Privacy, encrypts the data transmitted in wireless mode between two devices to prevent the unauthorized user to bug or invade the wireless network.

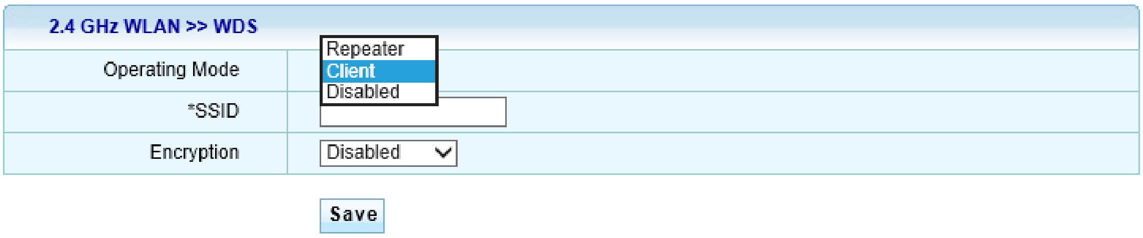
WPA: short for Wi-Fi Protected Access, has the WPA and WPA2 standards and protects the Wi-Fi security. It is generated based on several serious weaknesses found in the last generation of system WEP by the researcher.

(5) Authentication: specifies the authentication type. Two types are available, Personal (Pre-shared Key) and Enterprise (Radius). When

Personal is chosen, enter a key with 8~63 characters. When Enterprise is chosen, a Radius server will be needed.

2.4.3 WDS

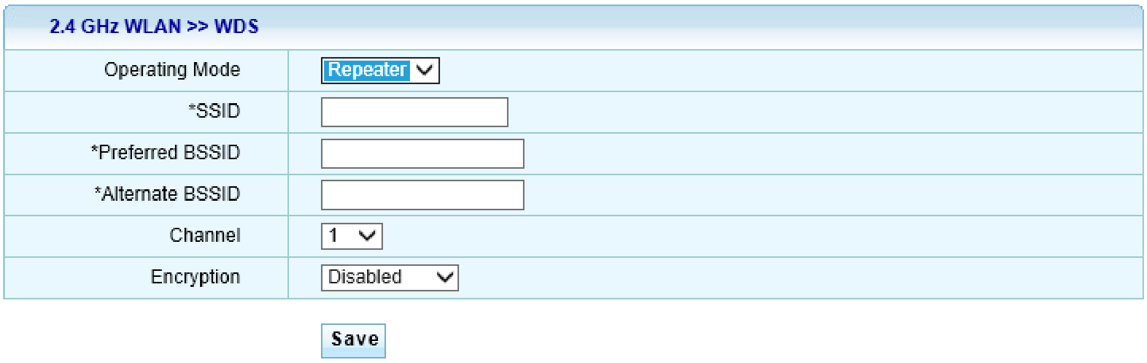
On this page, you could set different modes to bridge and connect to other wireless Access Point while still keeps the two WLANs in the same network, shown as Figure 2-15 and 2-16.



2.4 GHz WLAN >> WDS

Operating Mode	Repeater Client Disabled
*SSID	
Encryption	Disabled

Figure 2-15 Client Mode



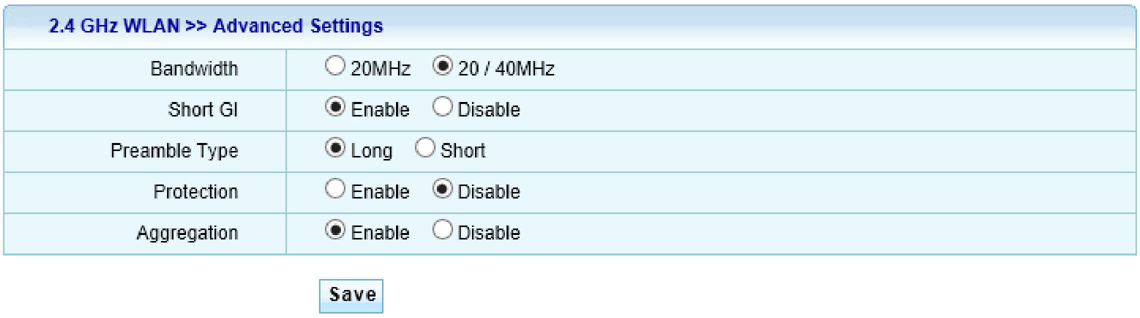
2.4 GHz WLAN >> WDS

Operating Mode	Repeater
*SSID	
*Preferred BSSID	
*Alternate BSSID	
Channel	1
Encryption	Disabled

Figure 2-16 Repeater Mode

Operating Mode: there are three options available: ***Repeater***, ***Client***, *and* ***Disabled***. When choosing Repeater or Client, the Wireless parameters of which you want to connect to should be filled in, including SSID, Encryption, Channel(for Repeater).

2.4.4 Advanced Setting



2.4 GHz WLAN >> Advanced Settings

Bandwidth	○ 20MHz ● 20 / 40MHz
Short GI	● Enable ○ Disable
Preamble Type	● Long ○ Short
Protection	○ Enable ● Disable
Aggregation	● Enable ○ Disable

Figure 2-17 The advanced setting interface

(1) **Bandwidth**: can be set to **20MHz** or **40MHz**. **40MHz** here indicates the coexistence of 20MHz and 40MHz.

(2) **Short GI**: can be set to **Enable** or **Disable**. GI indicates the transmission interval of the data block. A short GI results in faster transmission rate and also high probability of error, especially in the multipath effect environment.

(3) **Preamble Type**: can be set to **Long** or **Short**. The 802.11 frame contains three parts: preamble, header, and payload. When the preamble is short, the transmission rate is high, but the compatibility may be poor.

(4) **Protection**: can be set to **Enable** or **Disable**. Protection, b/g Protection, indicates the protection mode of 802.11b. Because the work modes of b, g, and n are different, the entire network efficiency will be greatly reduced if the 802.11b protection is enabled.

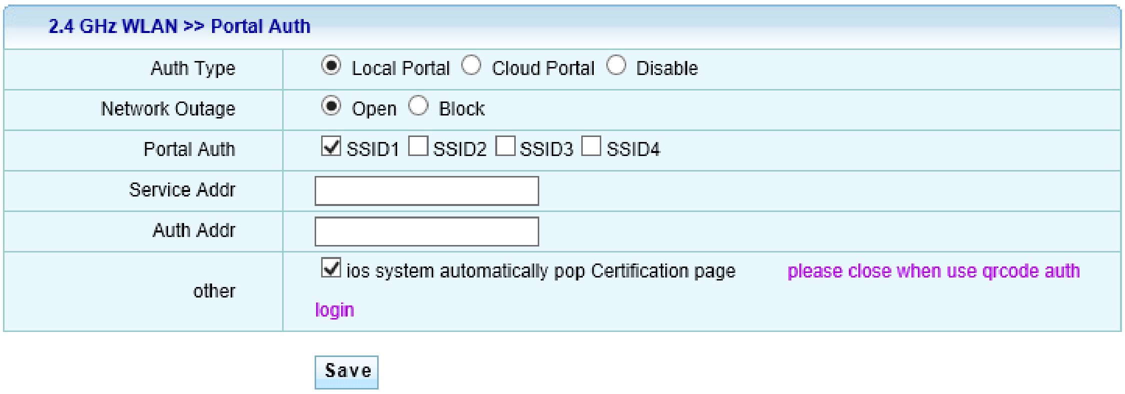
(5) **Aggregation**: can be set to **Enable** or **Disable**. Combining multiple data frames as one frame can obviously improve the network efficiency.

In addition, the relationship among the bandwidth, short GI, and Max Tx rate can be simply explained in the following mode.

Bandwidth	short GI	Max TX Rate
20	Enable	150 Mbps
20	Disable	135 (130) Mbps
40	Enable	300 Mbps
40	Disable	270 Mbps

2.4.5 Portal Authentication

On the **Portal Auth** interface, you can configure the portal authentication function of the AP, as shown in Figure 2-18.



2.4 GHz WLAN >> Portal Auth

Auth Type	● Local Portal ○ Cloud Portal ○ Disable
Network Outage	● Open ○ Block
Portal Auth	☑ SSID1 □ SSID2 □ SSID3 □ SSID4
Service Addr	
Auth Addr	
other	☑ ios system automatically pop Certification page please close when use qrcode auth login

Figure 2-18 The portal authentication interface

(1) **Auth Type**: Specifies the Portal type as Local or Cloud Portal. Disable means no portal authentication will be used.

(2) **Network Outage**: it specifies how AP would work when AP fails to communicate with AC. When set as *OPEN*, AP will allow clients' data to pass; when set as *BLOCK*, AP will NOT allow clients' data to pass.

(3) **Portal Auth**: specifies which SSID(s) will enable portal auth function.

(4) **Service Addr**: specifies the IP address of the AC.

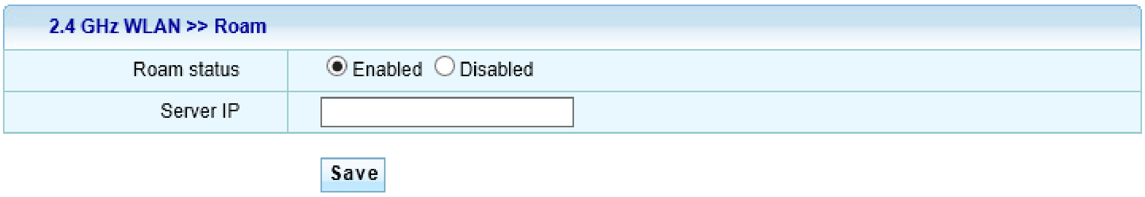
(3) **Auth Addr**: specifies the IP address of the AC generally. The IP address must be in the same network segment of the gateway address. For example, if the gateway address is 192.168.1.1, then the IP address must be 192.168.1.X.

(4) **Others**: specifies how certification page will pop up on iOS.

Notes: The portal function can be enabled or disabled for different SSIDs.

2.4.6 Roam

When Roam function is enabled, Serer IP should be filled in, as shown in Figure 2-19.



2.4 GHz WLAN >> Roam

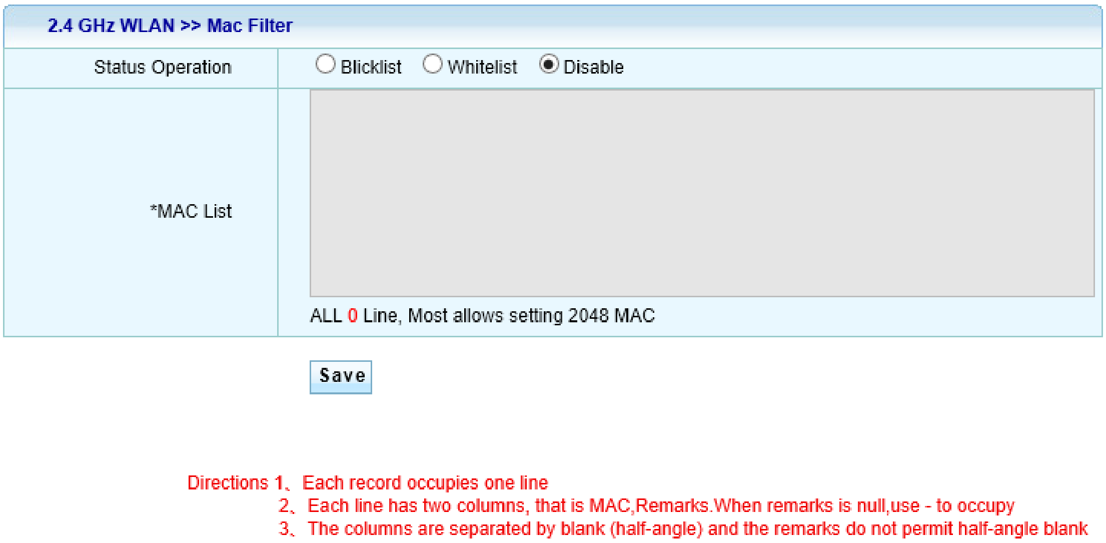
Roam status	● Enabled ○ Disabled
Server IP	

Figure 2-19 Roam Page

2.4.7 MAC Filtering

On the **MAC Filter** interface, you can configure the MAC filtering function of the AP.

Choose **WEB Management** > **2.4GHz WLAN** > **MAC Filter** to enter the **MAC Filter** interface, as shown in Figure 2-20.



2.4 GHz WLAN >> Mac Filter

Status Operation	○ Blicklist ○ Whitelist ● Disable
*MAC List	ALL 0 Line, Most allows setting 2048 MAC

Directions 1、Each record occupies one line
2、Each line has two columns, that is MAC,Remarks.When remarks is null,use - to occupy
3、The columns are separated by blank (half-angle) and the remarks do not permit half-angle blank

Figure 2-20 The MAC filtering interface

(1) **Status Operation**: specifies the filtering rule for the content in the MAC list. **Blacklist** indicates that the content is blocked and **Whitelist** indicates that the content is allowed.

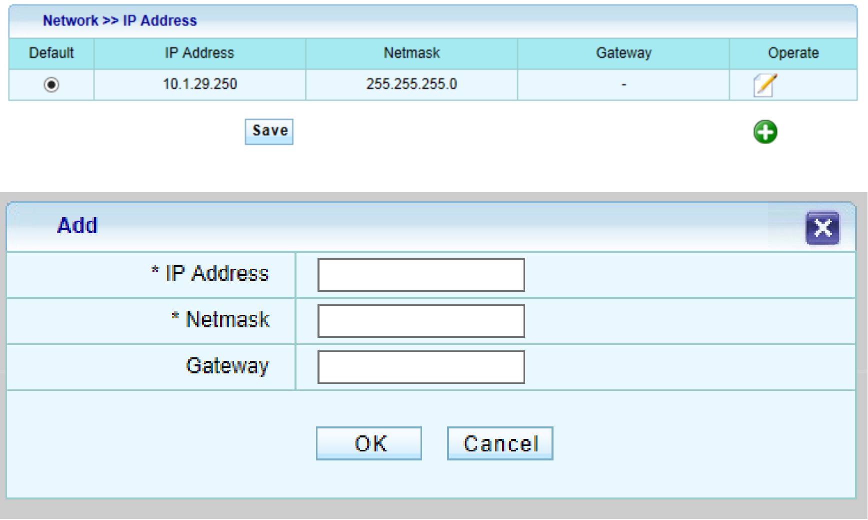
(2) **MAC List**: fills the MAC information to be filtered.

2.5 Network Configuration

2.5.1 IP Address

On the **IP Address** interface, you can configure the IP address, subnet mask, and gateway of the AP. Through these functions, you can specify the AP to register on a certain AC. If the AP and AC do not exist in the same LAN, the gateway and IP address of the AP need to be filled. If the AP and AC exist in the same LAN, the information can be omitted.

Choose **WEB Management** > **Network** > **IP Address** to enter the **IP Address** interface, as shown in Figure 2-21.



Network >> IP Address

Default	IP Address	Netmask	Gateway	Operate
●	10.1.29.250	255.255.255.0	-	

Add

* IP Address	
* Netmask	
Gateway	

Figure 2-21 The IP address interface

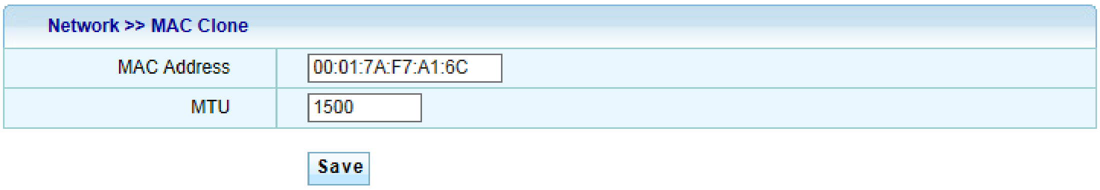
(1) **IP Address**: specifies the IP address of the AP manually.

(2) **Netmask**: specifies the subnet mask of the LAN in which the specified AC locates.

(3) **Gateway**: specifies the gateway address of the LAN in which the AC locates.

2.5.2 MAC Clone

This function allows the user to modify the MAC address and MTU value of the AP. This function is usually used before the old AP replaces the new AP to prevent causing a series of problems due to MAC address changing. The MAC address of the old AP can be copied to the new AP. Generally, **MTU** is set to the default value and do not need to be modified.



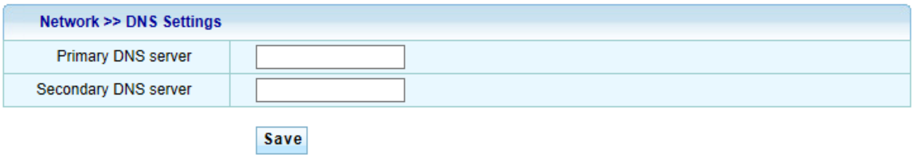
Network >> MAC Clone

MAC Address	00:01:7A:F7:A1:6C
MTU	1500

Figure 2-22 The MAC clone interface

2.5.3 DNS Setting

This function allows the user to modify the DNS configuration information of the AP and is usually used for the tracert detection function of the AP.

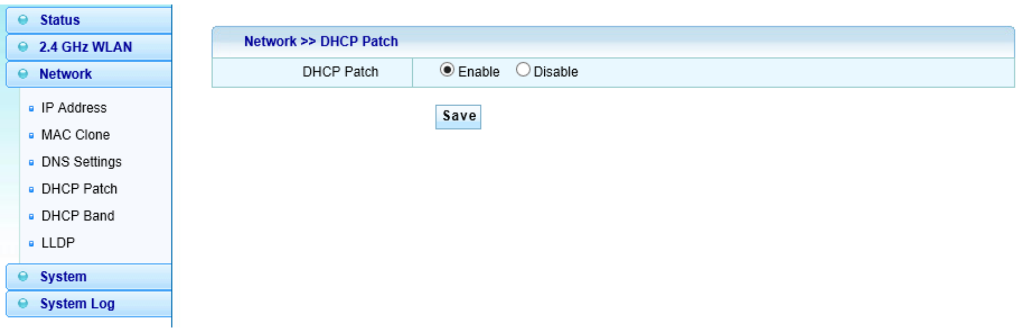


Network >> DNS Settings

Primary DNS server	
Secondary DNS server	

Figure 2-23 The DNS setting interface

2.5.4 DHCP Patch



Network >> DHCP Patch

DHCP Patch ● Enable ○ Disable

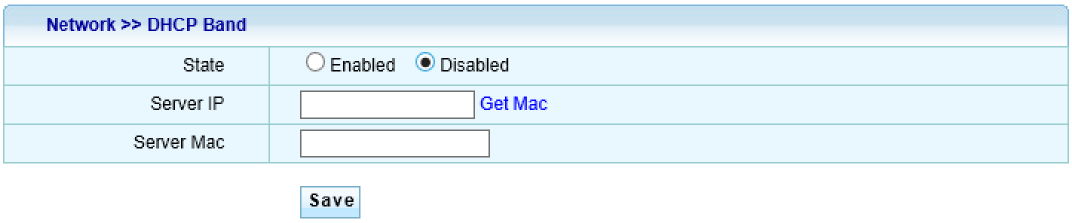
Figure 2-24 The DHCP patch interface

For some operating systems, such as Win7 and Mac OS X, the WLAN clients only receive the unicast DHCP packets, and do not receive the broadcast DHCP packets. Therefore, the DHCP patch function is added to the AP to solve the problem that some systems cannot obtain the IP address.

2.5.5 DHCP Band

When enabled, DHCP packet will only send to the specified DHCP Sever specified here.

Note: AP would use unicast instead of broadcast packet when it's enabled. Make sure the DHCP server would accept the DHCP unicast packet.



Network >> DHCP Band

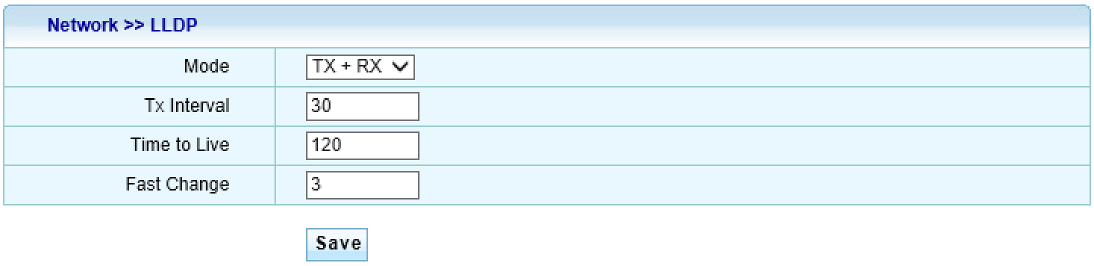
State	○ Enabled ● Disabled
Server IP	Get Mac
Server Mac	

Figure 2-25 DHCP Band

2.5.6 LLDP

The Link Layer Discovery Protocol or LLDP is a vendor-neutral Layer 2 protocol that allows a network device to advertise its identity and capabilities on the local network.

On this LLDP Page, you could change the parameters including **Mode**, **Tx Interval**, **Time to Live** and **Fast Change**.

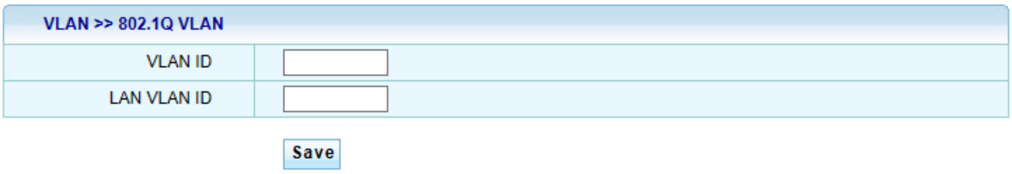

Network >> LLDP

Mode	TX + RX
Tx Interval	30
Time to Live	120
Fast Change	3

Figure 2-26 LLDP

2.6 VLAN Configuration

2.6.1 802.1Q VLAN


VLAN >> 802.1Q VLAN

VLAN ID	
LAN VLAN ID	

Figure 2-27 The 802.1Q VLAN interface

(1) **VLAN ID**: If the AC manages the AP in the LAN, the VLAN ID of the AC must be added and the AC can communicate with the AP and manages the AP.

(2) **LAN VLAN ID**: fills the VLAN ID to be allocated to the AP.

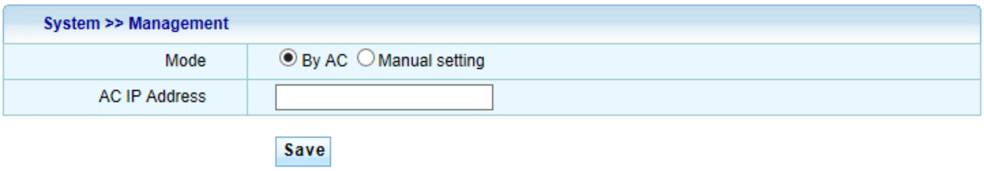
Notes:

Only when **Mode** is set to **Manual setting**, the **VLAN** option is available.

2.7 System Setting

2.7.1 Management Mode

Choose **WEB Management** > **System** > **Management** to enter the **Management** interface, as shown in Figure 2-28.



System >> Management

Mode	● By AC ○ Manual setting
AC IP Address	

Figure 2-28 The management mode interface

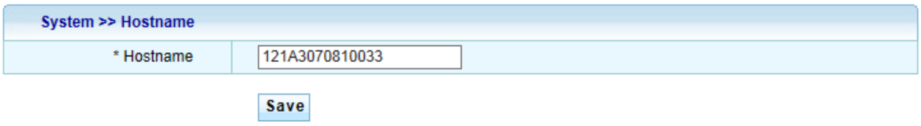
(1) **By AC**: **Mode** for the AP is set to **By AC** by default. When the AP starts, the AP will automatically search the wireless AC in the LAN, register on the AC automatically, and download default template configuration from the AC, and the configuration takes effect immediately. For details, refer to the AP template description in the AC manual.

(2) **Manual Setting**: when the AP needs to be managed independently, enable the **Manual setting**. When this setting is enabled, you can modify the wireless parameters on the AP web page.

(3) **Save**: Click **Save** after filling the AP static configuration to enable the parameter to take effect.

2.7.2 Host Name

On the **Hostname** interface, you can change the host name of the AP. **Hostname** is set to the SN of the AP by default, as shown in Figure 2-29.



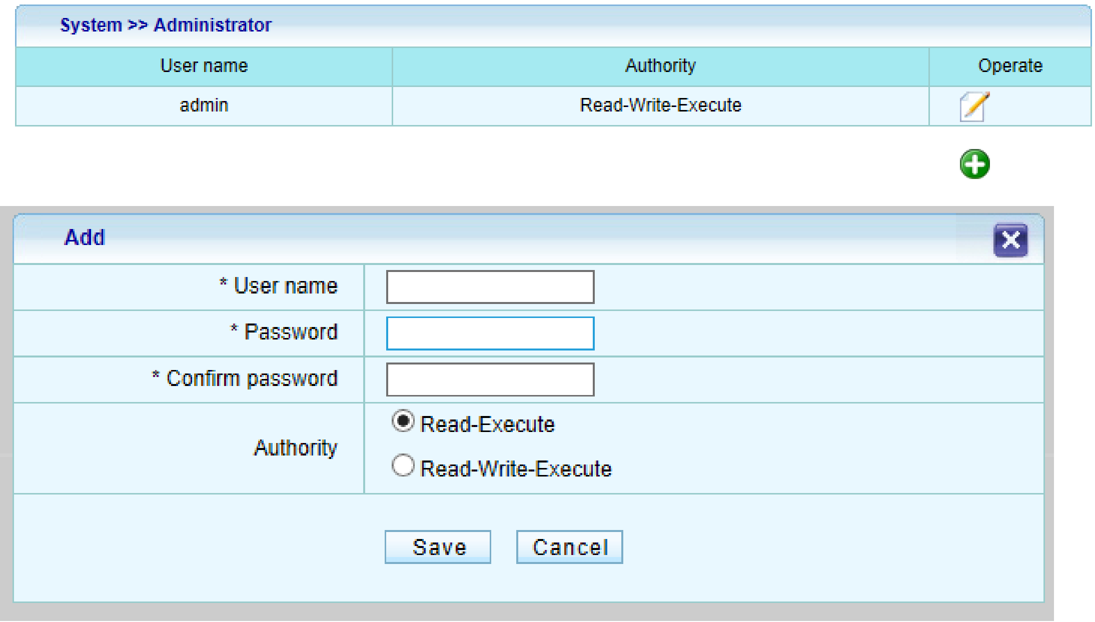
System >> Hostname

* Hostname	121A3070810033

Figure 2-29 The host name interface

2.7.3 Administrator Setting

On the **Administrator** interface, you can set the user name, password, and administrative authority of the user for logging in to the web management page. Choose **WEB Management** > **System** > **Administrator** to enter the **Administrator** interface, as shown in Figure 2-30.



System >> Administrator

User name	Authority	Operate
admin	Read-Write-Execute	

Add

* User name	
* Password	
* Confirm password	
Authority	● Read-Execute ○ Read-Write-Execute

Figure 2-30 The administrator setting interface

(1) **User name**: specifies the user name for the user logging in to the system.

(2) **Password**: specified the password for the user logging in to the system.

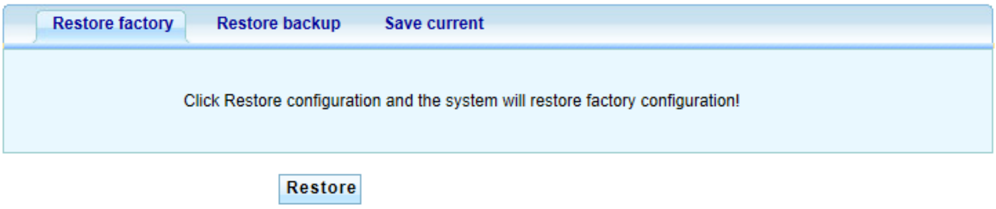
(3) **Confirm password**: specifies the password conformation and must be identical to the previously inputted password.

(4) **Authority**: specifies the authority for the user operating the system.

2.7.4 Profiles

On the **Profile** interface**,** you can choose **Restore factory**, **Restore backup**, and **Save current**.

Choose **WEB Management** > **System** > **Profiles** to enter the **Restore factory**, **Restore backup**, and **Save current** interfaces, as shown in Figure 2-31.



Click Restore configuration and the system will restore factory configuration!

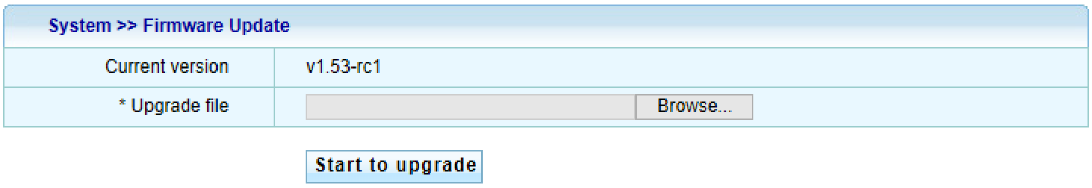
Figure 2-31 The configuration file interface

Restore configuration: click to restore to the default configuration.

2.7.5 Firmware Upgrade

Firmware upgrade is a necessary function for the network product. The software must be optimized and upgraded continuously to satisfy the changeable network environment and meet different requirements. Whether the software upgrade can be promoted to meet the changeable requirements is more and more concerned by users.

Choose **WEB Management** > **System** > **Firmware Update** to enter the **Firmware Update** interface, as shown in Figure 2-32.



Current version	v1.53-rc1
* Upgrade file	

Figure 2-32 The firmware upgrade interface

Current version: displays the software version number used by the current system.

Upgrade file: specifies the software package for upgrading the system, which is provided by the manufacturer.

Notes:

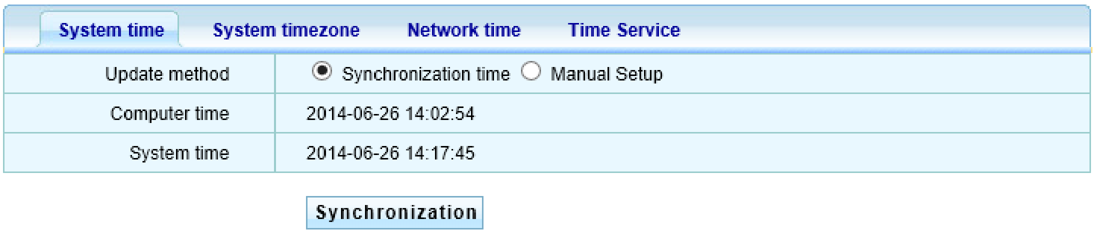
1) All the options with asterisk (*) are mandatory.

2) There is risk for firmware upgrading. Do not pause during the upgrading. The whole upgrading process will take about two minutes. A message will be prompted when the upgrade succeeds, therefore please wait patiently during the upgrading.

3) After the upgrade succeeds, reboot the AP manually to take the new version into effect. If the upgrade error message is prompted, do not reboot the AP and just repeat the upgrade operations until the upgrade succeeds. If the upgrade error occurs and the AP is powered off or the AP is powered off during upgrading, the system will fail to be started. In this case, contact the technical personnel for support.

2.7.6 System Time

On the **System time** interface, set the AP system time, as shown in Figure 2-33.



Update method	● Synchronization time ○ Manual Setup
Computer time	2014-06-26 14:02:54
System time	2014-06-26 14:17:45

Figure 2-33 The system time interface

(1) **Update method**: specifies the mode for modifying the time. It can be set to **Synchronization time** and **Manual Setup**.

(2) **Computer time**: specifies the time synchronous with the computer.

(3) **System time**: specifies the time displayed on the AP time setting interface.

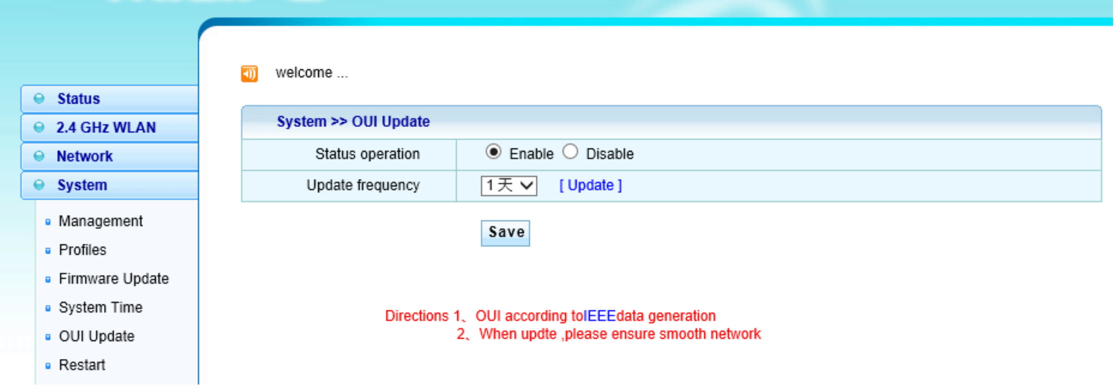
(4) **System timezone**: specifies the time zone in which the user locates.

(5) **Network time**: the AP will be automatically synchronized the time with the time server in a regular period.

(6) **Time service**: the user can choose whether to enable the time synchronization function.

2.7.7 OUI Update

You can update the OUI info by enabling OUI update on this page. The update frequency could also be configured here.



System >> OUI Update

Status operation: ● Enable ○ Disable

Update frequency: 1天 [Update]

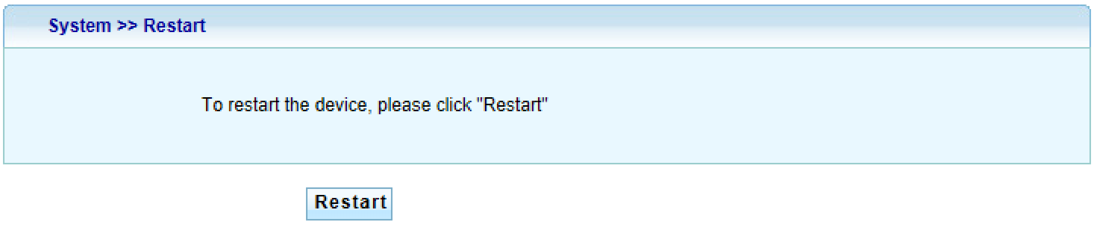
Directions 1、OUI according toIEEEdata generation
2、When updte ,please ensure smooth network

Figure 2-34 OUI Update

2.7.8 AP Restart

On the **Restart** interface, you can restart the AP.

Choose **WEB Management** > **System** > **Restart** to enter the **Restart** interface, as shown in Figure 2-35.



System >> Restart

To restart the device, please click "Restart"

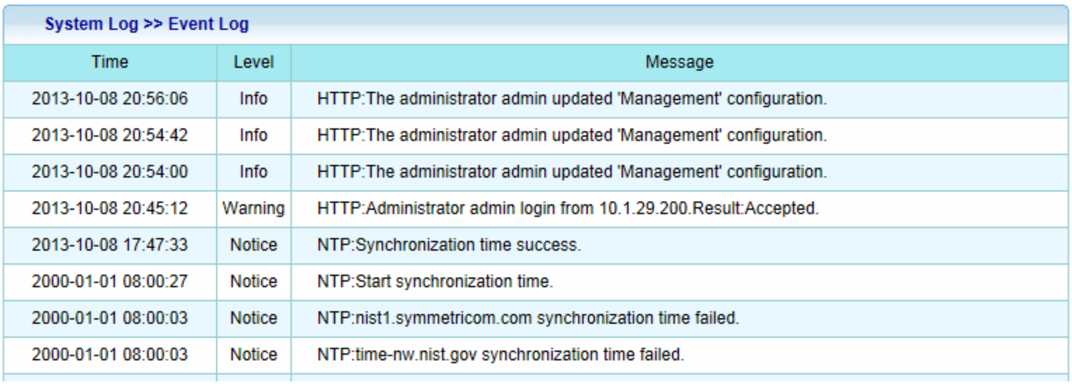
Figure 2-35 The restart interface

2.8 System Log

The AP running status is recorded and saved as a log to help us locate the fault, troubleshoot, and manage network security, and help us to analyze whether the AP is normal and whether the network is healthy.

2.8.1 Event Log

Choose **WEB Management** > **System Log** > **Event Log** to enter the **Event Log** interface, as shown in Figure 2-36.



System Log >> Event Log

Time	Level	Message
2013-10-08 20:56:06	Info	HTTP:The administrator admin updated 'Management' configuration.
2013-10-08 20:54:42	Info	HTTP:The administrator admin updated 'Management' configuration.
2013-10-08 20:54:00	Info	HTTP:The administrator admin updated 'Management' configuration.
2013-10-08 20:45:12	Warning	HTTP:Administrator admin login from 10.1.29.200.Result:Accepted.
2013-10-08 17:47:33	Notice	NTP:Synchronization time success.
2000-01-01 08:00:27	Notice	NTP:Start synchronization time.
2000-01-01 08:00:03	Notice	NTP:nist1.symmetricom.com synchronization time failed.
2000-01-01 08:00:03	Notice	NTP:time-nw.nist.gov synchronization time failed.

Figure 2-36 The event log interface

(1) **Time**: specifies the instant time when the system changes.

(2) **Level**: can be classified into **Info** and **Warning**. **Info** records the running events and **Warning** reminds you notice based on the running event recorded.

(3) **Message**: records the running event.

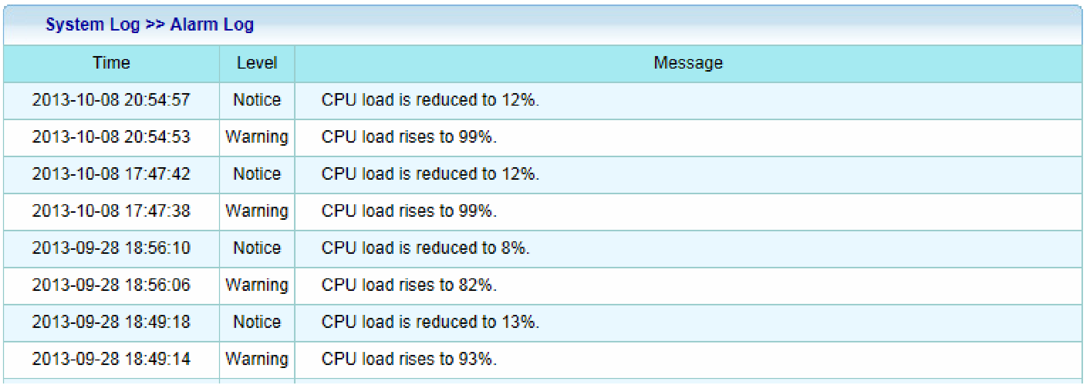
(4) **Refresh**: click **Refresh** to refresh the latest log information.

(5) **Clear**: click **Clear** to clear the log information.

(6) **Export**: click **Export** to export the log to a text.

2.8.2 Alarm Log

Choose **WEB Management** > **System Log** > **Alarm Log** to enter the **Alarm Log** interface, as shown in Figure 2-37.



System Log >> Alarm Log

Time	Level	Message
2013-10-08 20:54:57	Notice	CPU load is reduced to 12%.
2013-10-08 20:54:53	Warning	CPU load rises to 99%.
2013-10-08 17:47:42	Notice	CPU load is reduced to 12%.
2013-10-08 17:47:38	Warning	CPU load rises to 99%.
2013-09-28 18:56:10	Notice	CPU load is reduced to 8%.
2013-09-28 18:56:06	Warning	CPU load rises to 82%.
2013-09-28 18:49:18	Notice	CPU load is reduced to 13%.
2013-09-28 18:49:14	Warning	CPU load rises to 93%.

Figure 2-37 The alarm log interface

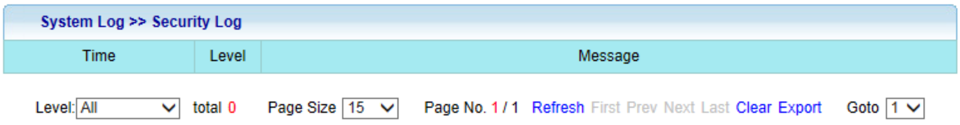
(1) **Time**: specifies the instant time when the system changes.

(2) **Level**: contains **Warning**. **Warning** reminds you notice.

(3) **Message**: records the running event.

2.8.3 Security Log

The security log contains the log tracing events, such as logging in to the system, change the visit authority, and start and shut down the system, as shown in Figure 2-38.



System Log >> Security Log

Time	Level	Message

Level: All total 0 Page Size 15 Page No. 1 / 1 Goto 1

Figure 2-38 The security log interface

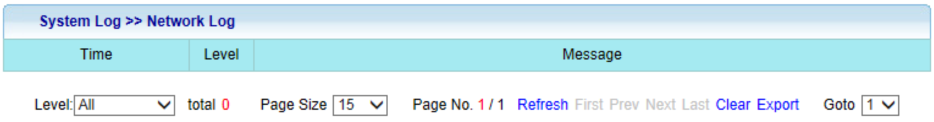
(1) **Time**: specifies the instant time when the system changes.

(2) **Level**: can be classified into **Info** and **Warning**. **Info** records the running events and **Warning** reminds you notice based on the running event recorded.

(3) **Message**: records the running event.

2.8.4 Network Log

Choose **WEB Management** > **System Log** > **Network Log** to enter the **Network Log** interface, as shown in Figure 2-39.



System Log >> Network Log

Time	Level	Message

Level: All total 0 Page Size 15 Page No. 1 / 1 Goto 1

Figure 2-39 The network log interface

(1) **Time**: specifies the instant time when the system changes.

(2) **Level**: can be classified into **Info** and **Warning**. **Info** records the running events and **Warning** reminds you notice based on the running event recorded.

(3) **Message**: records the running event.

Appendix

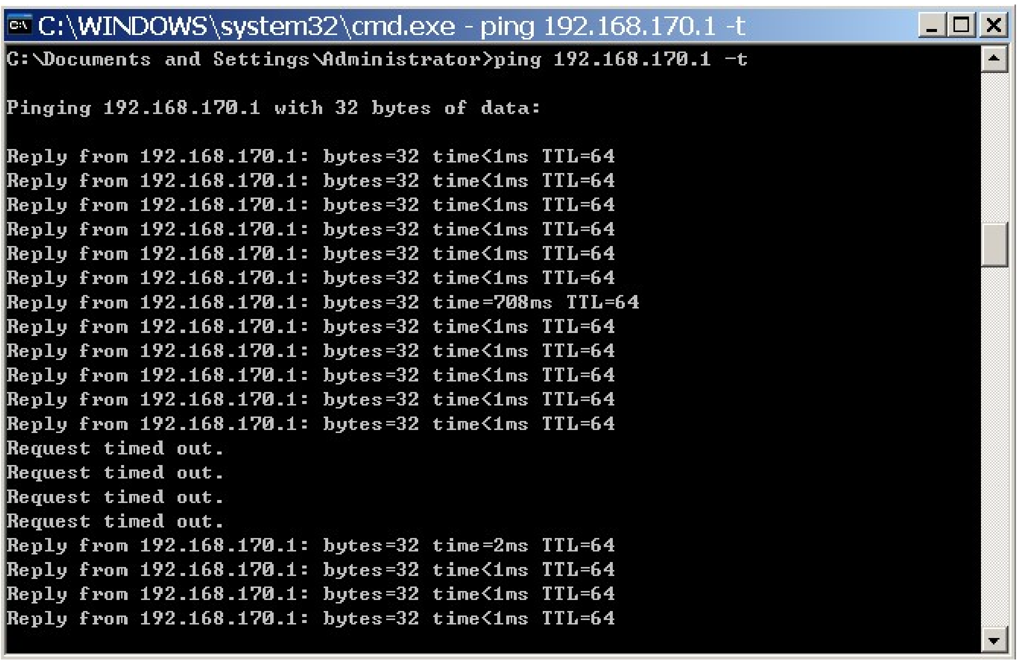
Hardware Restoration Configuration

If the AP password loss or other fault occurs, you can press the **Reset** button on the front panel to clear the configuration and restore the AP to the default setting.

Operation Steps:

Step 1: Power on the AP and start the AP to the normal work status. (The AP can be pinged through via the PC.)

Step 2: Use a sharp object to press the **Reset** button on the front panel and release the **Reset** button until the ping value is changed to a larger value, as shown in the following figure.



C:\WINDOWS\system32\cmd.exe - ping 192.168.170.1 -t

```
C:\Documents and Settings\Administrator>ping 192.168.170.1 -t

Pinging 192.168.170.1 with 32 bytes of data:

Reply from 192.168.170.1: bytes=32 time<1ms TTL=64
Reply from 192.168.170.1: bytes=32 time<1ms TTL=64
Reply from 192.168.170.1: bytes=32 time<1ms TTL=64
Reply from 192.168.170.1: bytes=32 time<1ms TTL=64
Reply from 192.168.170.1: bytes=32 time<1ms TTL=64
Reply from 192.168.170.1: bytes=32 time<1ms TTL=64
Reply from 192.168.170.1: bytes=32 time=708ms TTL=64
Reply from 192.168.170.1: bytes=32 time<1ms TTL=64
Reply from 192.168.170.1: bytes=32 time<1ms TTL=64
Reply from 192.168.170.1: bytes=32 time<1ms TTL=64
Reply from 192.168.170.1: bytes=32 time<1ms TTL=64
Reply from 192.168.170.1: bytes=32 time<1ms TTL=64
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.170.1: bytes=32 time=2ms TTL=64
Reply from 192.168.170.1: bytes=32 time<1ms TTL=64
Reply from 192.168.170.1: bytes=32 time<1ms TTL=64
Reply from 192.168.170.1: bytes=32 time<1ms TTL=64
```

Step 3: Enable the AP to reboot automatically. The system restores the default configuration when the AP is rebooted normally.

Notes:

(1) This function will take effect when the AP is started normally. (The AP can be pinged through via the PC.)

(2) Press the **Reset** button and do not release in the midway.

(3)Contact the technical personnel for support if the system does not work normally.